Claims:

1. A method of transmitting data using encryption between a sender and a receiver, the method comprising:

generating a first encryption key unknown to the receiver;

encrypting said data to be transmitted from the sender to the receiver using said first key;

providing separate Second Information Processing Systems (SIPSs) in secure local communication with both the sender and the receiver;

the sender transmitting to its SIPS the first encryption key and information dependent on an identity of the receiver;

the SIPS of the sender selecting one of a plurality of second keys corresponding to the information dependent on the identity of the receiver and a unique identifier corresponding to said selected second key, said identifier and said corresponding selected second key being known to the SIPS of the receiver;

the SIPS of the sender encrypting the first encryption key using the selected second key to provide an encrypted first key;

the SIPS of the sender encrypting said identifier corresponding to said selected second key using a third encryption key allowing the sender to retrieve said identifier to provide an encrypted identifier;

transmitting said encrypted first key, said encrypted identifier and said data to be transmitted from the sender to the receiver using said first key over a generally unsecured transmission link;

transmitting from the receiver to the SIPS of the receiver said encrypted first key and said encrypted identifier;

the SIPS of the receiver decrypting said encrypted identifier using the third encryption key to retrieve from the SIPS device of the receiver the second encryption key;

the SIPS of the receiver decrypting said encrypted first key using said second encryption key to provide the receiver with the first encryption key; and

the receiver decrypting said data using said the retrieved first encryption key.

2. An information process arrangement comprising a First Information Processing System (FIPS) and a Second Information Processing System (SIPS) arranged separate from the FIPS and capable of exchanging signals with the FIPS, wherein

the FIPS comprises

-FIPS key generation means to generate a first key;

-FIPS encryption means to encrypt sensitive data using the first key, thereby generating temporarily secured sensitive data;

-FIPS correspondent selection means to select correspondent data to which the sensitive data is destined; and

-FIPS storage means to store temporarily secured sensitive data;

the SIPS comprises

-SIPS storage means to store correspondence data, a plurality of keys, a plurality of key identifiers, and a public key;

-SIPS identification means to identify a correspondent key and a correspondent key identifier based on received FIPS selected correspondent data; and

-SIPS encryption means to encrypt FIPS received first key using said identified correspondent key, and to encrypt correspondent key identifier using said public key, thereby generating a secured first key and a secured key identifier; and

the FIPS further comprises

-FIPS secured data integration means to integrate into temporarily secured sensitive data, received SIPS secured first key and secured key identifier into integrated secured sensitive data.

3. The information process arrangement of claim 2, further comprising authentication means receiving user provided authentication data which is compared with SIPS stored authentication data in order to grant or deny SIPS use.

4. The information processing arrangement of claim 2, wherein the SIPS further comprises integration means to integrate SIPS encrypted data in a single signal communicated to the FIPS.

5. The information processing arrangement of claim 2, wherein the FIPS further comprises at least one of:

-communication control means to close external communication when a securing sensitive data process is initiated;

-anti-spy means to prevent undesired means to record signal exchanged between the FIPS and the SIPS; and

-automatic deletion means to erase from the FIPS at least one of unsecured, FIPS secured and SIPS secured data else that integrated secured sensitive data one the integrated secured sensitive data has been generated.

6. The information processing arrangement of claim 2, wherein the SIPS further comprises puzzling means that complete at least one of:

-creating unnecessary signals between valuable signals transmitted to the FIPS; and

-modifying SIPS generated signals and data transmitted to the FIPS in order to render more difficult the reading of said signals and data.

7. The information processing arrangement of claim 2, wherein a second processing arrangement having a SIPS component having stored correspondent key and associated correspondent key identifier corresponding to the information processing arrangement SIPS stored selected correspondent key and correspondent key identifier is necessary to decrypt the integrated secured sensitive data generated by the information processing arrangement.

8. The information processing arrangement of claim 2, wherein the FIPS is a data processing system including communication capability and the FIPS is a smart card comprising computing capability.

9. An information process arrangement comprising a First Information Processing System (FIPS) and a Second Information Processing System (SIPS) arranged separate from the FIPS and capable of exchanging signals with the FIPS, wherein

the FIPS comprises

-FIPS storage means to store integrated secured sensitive data; and

-FIPS secured data extraction means to extract from integrated secured sensitive data a secured first key, a secured key identifier, and temporarily secured sensitive data;

the SIPS comprises

-SIPS storage means to store correspondence data, a plurality of keys, a plurality of key identifiers, and a public key; and

-SIPS decryption means to decrypt FIPS received secured key identifier using the public key, thereby extracting the correspondent key identifier, to decrypt FIPS received secured first key using the key corresponding in the SIPS storage means to extracted key identifier, thereby extracting the first key; and

the FIPS further comprises

-FIPS decryption means to decrypt temporarily secured sensitive data using the SIPS received first key, therefore extracting the sensitive data.

10. The information process arrangement of claim 9, further comprising authentication means receiving user provided authentication data which is compared with SIPS stored authentication data in order to grant or deny SIPS use.

11. The information processing arrangement of claim 9, wherein the FIPS further comprises at least one of:

-communication control means to close external communication when a securing sensitive data process is initiated;

-anti-spy means to prevent undesired means to record signal exchanged between the FIPS and the SIPS; and

-automatic deletion means to erase from the FIPS at least one of extracted secured key identifier, extracted secured first key, first key, and extracted temporarily secured sensitive data.

12. The information processing arrangement of claim 9, wherein the SIPS further

comprises puzzling means that complete at least one of:

-creating unnecessary signals between valuable signals transmitted to the FIPS; and

-modifying SIPS generated signals and data transmitted to the FIPS in order to render more difficult the reading of said signals and data.

13. The information processing arrangement of claim 9, wherein the FIPS is a data processing system including communication capability and the FIPS is a smart card comprising computing capability.

14. An Information Processing System (IPS) comprising:

-storage means to store correspondence data, a plurality of keys, a plurality of key identifiers, and a public key;

-input means to receive from an external IPS a correspondent signal and a first key used by said external IPS to encrypt sensitive data;

-selection means to identify a correspondent key and a correspondent key identifier corresponding to the received correspondent signal in the storage means;

-encryption means to encrypt the first key using said identified correspondent key, and to encrypt correspondent key identifier using said public key, thereby generating a secured first key and a secured key identifier; and

-outputting means to transmit the secured first key and the secured key identifier to the external IPS as to said external IPS to store the encrypted sensitive data, the secured first key and the secured key identifier into integrated data.

15. The IPS of claim 14, further comprising correspondent association means allowing to individually associate a key and a key identifier with correspondent data in the IPS storage means.

16. The IPS of claim 14, further comprising puzzling means that complete at least one of:

-creating unnecessary signals between valuable signals transmitted to the FIPS; and

-modifying SIPS generated signals and data transmitted to the FIPS in order to render

more difficult the reading of said signals and data.

17. The IPS of claim 14, wherein a secondary IPS having stored correspondent key and associated correspondent key identifier corresponding to the IPS stored selected correspondent key and correspondent key identifier is necessary to decrypt the secured key identifier and secured first key, thereby extracting the first key.

18. The IPS of claim 14, embodied in a smart card.

19. An Information Processing System (IPS) comprising:

-storage means to store correspondence data, a plurality of keys, a plurality of key identifiers, and a public key;

-input means to receive from an external IPS a secured first key and a secured key identifier extracted from integrated secured sensitive data by said external IPS;

-decryption means to decrypt the secured key identifier using the public key, thereby extracting a correspondent key identifier, and to decrypt the secured first key using an identified correspondent key, thereby extracting a first key;

-selection means to identify a correspondent key corresponding to the extracted correspondent key identifier in the storage means; and

-outputting means to transmit the first key to the external IPS as to said external IPS to decrypt integrated secured sensitive data using said first key, thereby extracting the sensitive data.

20. The IPS of claim 19, further comprising correspondent association means allowing to individually associate a key and a key identifier with correspondent data in the IPS storage means.

21. The IPS of claim 19, further comprising puzzling means that complete at least one of:

-creating unnecessary signals between valuable signals transmitted to the FIPS; and

-modifying SIPS generated signals and data transmitted to the FIPS in order to render

more difficult the reading of said signals and data.

22. The IPS of claim 19, embodied in a smart card.

23. An information process arrangement comprising a plurality of Information Processing Systems (IPSs) completing at least one of encrypting and decrypting a first key used for the encryption of sensitive data exchanged between two external information processing systems with pairing of an encryption participating IPS with a decryption participating IPS being required for the decryption participating IPS to decrypt the first key encrypt by the encryption participating IPS, the IPSs being communicatively linked and capable of exchanging signals, wherein each IPS comprises

-storage means to store a public key, correspondent data, a plurality of keys, and a plurality of key identifiers;

-selection means to identify a key and a key identifier in the storage means;

-ciphering means to generate availability codes based on identified key and key identifier;

-communication means to exchange availability codes with another IPS;

-verification means to compare received availability codes with keys and key identifiers stored in storage means;

-correspondence setting means to associate identified key and key identifier to correspondent data, whereby two IPSs exchanging availability codes complete a correspondence pairing process.

24. The information process arrangement of claim 23, wherein an IPS further comprises authentication means receiving user provided authentication data which is compared with IPS stored authentication data in order to grant or deny IPS use.

25. The information process arrangement of claim 23, wherein the IPSs further comprise code generation means to generate codes based on at least one of user provided information and other IPS provided data to complete at least one of other IPS authentication and

generation of availability codes with the IPS ciphering means using the code generation means generated codes.

26. The information processing arrangement of claim 23, wherein the IPSs further comprise correspondent association means individually associating a key and a key identifier with correspondent data in the IPS storage means.

27. The information processing arrangement of claim 23, further comprising key identifier generation means to generate a unique key identifier.

28. An Information Processing System (IPS) completing at least one of encrypting and decrypting a first key used for the encryption of sensitive data exchanged with another IPS and wherein the decryption of the first key requires a correspondent pairing of the encrypting IPS with the decrypting IPS, wherein the IPS comprises

-storage means to store a public key, correspondent data, a plurality of keys, and a plurality of key identifiers;

-selection means to identify a key and a key identifier in the storage means;

-ciphering means to generate availability codes based on identified key and key identifier;

-communication means to exchange availability codes with another IPS;

-verification means to compare received availability codes with keys and key identifiers stored in storage means;

-correspondence setting means to associate identified key and key identifier to correspondent data, whereby a correspondence pairing process is completed between the ISP and said other ISP.

29. The IPS of claim 28, further comprising authentication means receiving user provided authentication data to compare with IPS stored authentication data in order to grant or deny IPS use.

30. The IPS of claim 28, further comprising code generation means to generate codes based on at least one of user provided information and other IPS provided data to complete at least one of other IPS authentication and generation of availability codes with the IPS ciphering means using the code generation means generated codes.

31. The IPS of claim 28, further comprising correspondent association means individually associating a key and a key identifier with correspondent data in the IPS storage means.

32. The IPS of claim 28, further comprising correspondent receiving data means to receive correspondent data for the correspondent setting means to store the correspondent data in the storage means during the correspondent pairing process.

33. The IPS of claim 28, further comprising puzzling means that complete at least one of:

-creating unnecessary signals between valuable signals transmitted by the IPS; and

-modifying transmitted IPS generated signals and data in order to render more difficult the reading of said signals and data.

34. The IPS of claim 28, further comprising key identifier generation means to generate at least one key identifier.

35. The IPS of claim 28, embodied in a smart card.

36. An information processing method comprising:

-generating a first key in a First Information Processing System (FIPS);

-encrypting sensitive data using the generated first key, thereby generating temporary secured sensitive data;

-selecting a correspondent to whom the sensitive data is destined;

-transmitting the first key and correspondent selection data from the FIPS to a Second Information Process System (SIPS) which is arranged separate from the FIPS;

-identifying among SIPS stored key identifiers and keys a correspondent key identifier and a correspondent key based on received correspondent selection data from the FIPS;

-encrypting the first key using the identified correspondent key, thereby generating a secured first key in said SIPS;

-encrypting the identified correspondent key identifier using a SIPS stored public key, thereby generating a secured key identifier in said SIPS;

-transmitting the secured first key and the secured key identifier from the SIPS to the FIPS; and

-integrating into integrated secured sensitive data the temporarily secured data, the secured first key, and the key identifier.

37. The method of claim 36, further comprising authenticating a user and granting SIPS use to the user.

38. The method of claim 36, further comprising at least one of:

-storing integrated secured data on accessible holding means; and

-communicating integrated secured data to a correspondent FIPS.

39. The method of claim 36, further comprising erasing the first key, the temporarily secured sensitive data, and the SIPS communicated secured key and secured key identifier from the FIPS.

40. The method of claim 36, further comprising puzzling communication between the SIPS and the FIPS by at least one of:

-creating unnecessary signals between valuable signals transmitted to the FIPS; and

-modifying SIPS generated signals and data transmitted to the FIPS in order to render more difficult the reading of said signals and data.

41. An information processing method comprising:

-extracting from integrated secured sensitive data a secured first key and a secured key identifier on a First Information Processing System (FIPS);

-transmitting the secured first key and the secured key identifier from the FIPS to a Second Information Processing System (SIPS) separate from the FIPS;

-decrypting the key identifier using a SIPS stored public key on the SIPS, thereby extracting a correspondent key identifier;

-identifying a correspondent key associated to the identified correspondent key identifier among SIPS stored keys and key identifiers on the SIPS;

-decrypting the secured first key using the identified correspondent key on the SIPS, thereby extracting a first key;

-transmitting the first key from the SIPS to the FIPS; and

-decrypting the sensitive data using the first key on the FIPS, thereby extracting sensitive data.

42. The method of claim 41, further comprising authenticating a user and granting SIPS use to the user.

43. The method of claim 41, further comprising storing extracted sensitive data on FIPS storing means.

44. The method of claim 41, further comprising erasing FIPS extracted data from the FIPS.

45. An information processing method comprising:

-receiving from an external information processing system a first key used to encrypt sensitive data and correspondent data designating to whom the sensitive data is destined;

-identifying a correspondent key and a correspondent key identifier among stored keys and key identifiers using the received correspondent data;

-encrypting the received key using the identified correspondent key, thereby generating a secured first key;

-encrypting the identified correspondent key identifier using a stored public key, thereby generating a secured key identifier; and

-transmitting the secured first key and secured key identifier to the external information processing system for integration into integrated secured sensitive data.

46. The method of claim 45, further comprising authenticating a user and granting a method processing authorization to the user.

47. The method of claim 45, further comprising puzzling communication between the SIPS and the FIPS by at least one of:

-creating unnecessary signals between valuable signals transmitted to the FIPS; and

-modifying SIPS generated signals and data transmitted to the FIPS in order to render more difficult the reading of said signals and data.

48. An information processing method comprising:

-receiving from an external information processing system a secured first key and a secured key identifier extracted from integrated secured sensitive data;

-decrypting the secured key identifier using a stored public key, thereby extracting a correspondent key identifier;

-identifying an associated correspondent key based on correspondent key identifier among stored keys and key identifiers;

-decrypting the secured first key based on identified correspondent key, thereby extracting a first key; and

-transmitting the first key to the external information processing system for decryption of the integrated secured sensitive data, thereby extracting sensitive data.

49. The method of claim 48, further comprising authenticating a user and granting a method processing authorization to the user.

50. A correspondent pairing method between two Information Processing Systems (IPSs) storing a public key, correspondent data, a plurality of keys and a plurality of key identifiers, with each said IPS completing at least one of encrypting and decrypting a first key used for the encryption of sensitive data and wherein the decryption of the first key requires a correspondent pairing of the encrypting IPS with the decrypting IPS, the method comprising:

-establishing communication between the IPSs;

-identifying an available IPS stored key and key identifier among a plurality of stored keys and key identifiers on a primary IPS;

-generating ciphered availability codes based on identified key and key identifier on the primary IPS;

-exchanging the availability codes with the secondary IPS;

-verifying the key and the key identifier availability by comparing the exchanged ciphered availability codes with ciphered stored keys and key identifiers on the secondary IPS;

-setting correspondent data on the two IPSs when the exchanged availability codes identify an available key and key identifier on the two IPSs, whereby a correspondent pairing is created between the two IPSs.

51. The method of claim 50, further comprising authenticating a user and granting a method processing authorization to the user.

52. The method of claim 50, further comprising to receive at least one of user provided information and other IPS provided data to set correspondent data.

53. A correspondent pairing method for a primary Information Processing System (IPS) to set identical correspondent pairing data than at least one secondary IPS with the IPSs storing a public key, correspondent data, a plurality of keys and a plurality of key identifiers, with each said IPS completing at least one of encrypting and decrypting a first key used for the encryption of sensitive data and wherein the decryption of the first key requires a correspondent pairing of the encrypting IPS with the decrypting IPS, the method comprising:

-authenticating the secondary IPS;

-generating a ciphering seed common to the primary and the secondary IPS based on secondary IPS authentication;

-identifying an available IPS stored key and key identifier among a plurality of stored keys and key identifiers;

-generating ciphered availability codes based on the identified key and key identifier;

-transmitting the ciphered availability codes to the secondary IPS;

-receiving an availability code response from the secondary IPS;

-setting correspondent pairing data corresponding to the key and key identifier associated with a positive availability code response.

54. The method of claim 53, further comprising authenticating a user and granting a method processing authorization to the user.

55. The method of claim 53, further comprising receiving a user correspondent pairing type selection identifying at least the type of pairing as whether a single correspondent pairing or a group pairing.

56. A program storage device which stores program codes readable from a communication system in order to facilitate two Information Processing Systems (IPSs) to complete a correspondent pairing process, each IPS storing a public key, correspondent data, a plurality of keys and a plurality of key identifiers, with each said IPS completing at least one of encrypting and decrypting a first key used for the encryption of sensitive data and wherein the decryption of the first key requires a correspondent pairing of the encrypting IPS with the decrypting IPS, where in the program codes are responsible for the communication system complete the steps of:

-receiving user authorization to complete a correspondent pairing process;

-establishing communication between a primary IPS and a secondary IPS; and

-receiving user correspondent data.

57. The program storage device of claim 56, further comprising program codes responsible for the communication system to receive a user correspondent pairing type selection identifying at least the type of pairing as whether a single correspondent pairing or a group pairing.